USCYBERCOM

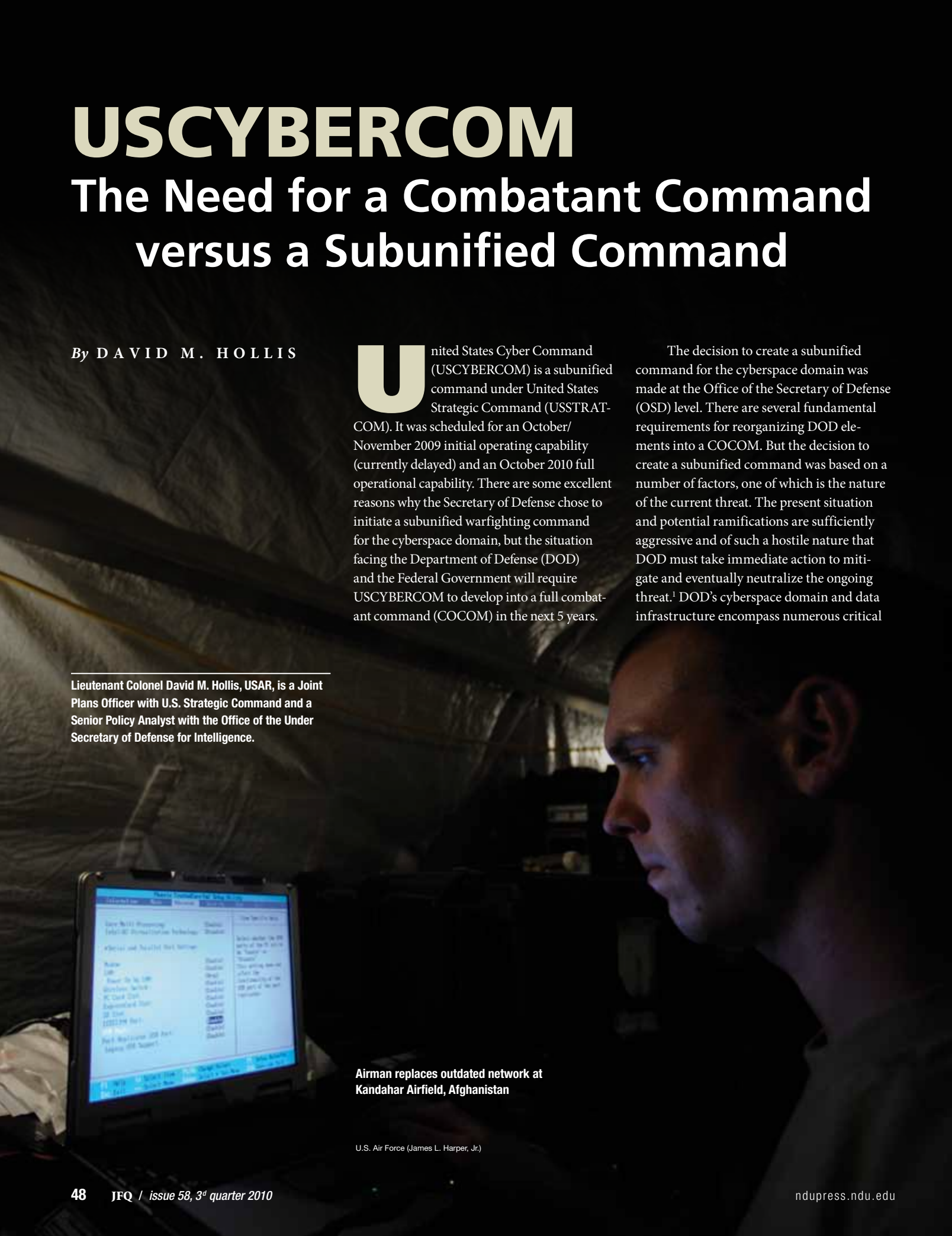
The Need for a Combatant Command versus a Subunified Command

By DAVID M. HOLLIS

United States Cyber Command (USCYBERCOM) is a subunified command under United States Strategic Command (USSTRATCOM). It was scheduled for an October/November 2009 initial operating capability (currently delayed) and an October 2010 full operational capability. There are some excellent reasons why the Secretary of Defense chose to initiate a subunified warfighting command for the cyberspace domain, but the situation facing the Department of Defense (DOD) and the Federal Government will require USCYBERCOM to develop into a full combatant command (COCOM) in the next 5 years.

The decision to create a subunified command for the cyberspace domain was made at the Office of the Secretary of Defense (OSD) level. There are several fundamental requirements for reorganizing DOD elements into a COCOM. But the decision to create a subunified command was based on a number of factors, one of which is the nature of the current threat. The present situation and potential ramifications are sufficiently aggressive and of such a hostile nature that DOD must take immediate action to mitigate and eventually neutralize the ongoing threat.[1] DOD's cyberspace domain and data infrastructure encompass numerous critical

Lieutenant Colonel David M. Hollis, USAR, is a Joint Plans Officer with U.S. Strategic Command and a Senior Policy Analyst with the Office of the Under Secretary of Defense for Intelligence.



Airman replaces outdated network at Kandahar Airfield, Afghanistan

U.S. Air Force (James L. Harper, Jr.)

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
USCYBERCOM: The Need for a Combatant Command versus a Subunified Command	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University Press,Joint Force Quarterly,260 Fifth Ave., Bldg. 64, Fort McNair,Washington,DC,20319-5066**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**6**	

vulnerabilities. OSD staff and congressional requirements for development of a full COCOM are difficult to achieve in the compressed timeframe as required by the threat and known vulnerabilities. Developing and focusing DOD's capability to conduct network warfare (NETWAR, as defined by the Army)[2] are urgent requirements. The reduced up-front effort to develop a subunified command would more quickly achieve DOD's immediate goal of a unified full-spectrum cyberwar capability. Additionally, internal DOD opposition to a full COCOM could extend the time required for its standup. Numerous COCOMs, Services, and agencies have developed their own NETWAR and cyberspace elements and want to maintain their independent capabilities. Yet these organizations are also looking to a unified authority to synchronize their own capabilities and plans.[3]

A subunified command under USSTRATCOM would effectively establish an intermediate goal toward the development of a full cyber COCOM, with a similar but reduced structure, mission, and authority compared to a full unified COCOM. The development of a subunified command is a rapid and effective step toward development of synchronized and focused DOD capabilities in cyberspace/NETWAR.

Cyberspace Definition and Warfighting Domain

Global cyberspace activity has occurred since the 19th century, when the telegraph, telephone, and radio created the first electronic information grid, matured into global interconnectivity, and permitted large-scale information exchange. The first electronic data transactions across early computer networks (Advanced Research Projects Agency Network/Military Network) evolved into what is today recognized as the Internet. Threats, vulnerabilities, and risks have grown exponentially with the proliferation of use and dependence on the cyberspace infrastructure. The electronic dependence of modern civilization on physical infrastructure (transport layer), massed data/information (storage, transmittal, and transaction), and the resulting critical infrastructure functionality (finance, health, utilities, government, and so forth) requires a seamless Internet environment. Consequently, cyberspace has become a warfighting domain with the inherent potential to destroy and/or render useless logical, physical, technical, and virtual infrastructure, and to damage critical national capabilities such as economic, government, military, educational, health, social, and other capabilities.

Cyberspace and its various definitions have been around since the 1980s.[4] In the *2006 National Military Strategy for Cyberspace Operations* (NMS–CO), the Joint Chiefs of Staff defined *cyberspace* as "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructures."[5] In contrast, the George W. Bush administration's

the electronic dependence of modern civilization requires a seamless Internet environment

2003 National Strategy to Secure Cyberspace does not use the word *data* in its definition: "Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security."[6] Various U.S. Government agencies now agree that cyberspace is a warfighting and operational domain, but what that actually means is unclear, and there are numerous other definitions.[7]

Elements of the cyberspace domain are common to the other warfighting domains; land, sea, air, and space are all interactive and require cross-domain planning, and cyberspace is no different. Cyberspace domain superiority supports freedom of action in all other domains and denies freedom of action to adversaries; it is a predicate to successful military operations. In addition, cyberspace offensive weapons have several analogies with nuclear/space forces. Their effects are global in nature—they cannot be contained to a specific geographic COCOM or theater. Cyberspace weapons, once used, lose their deterrent value and effectiveness because the opposing forces can immediately build counterdefenses.

However, military operations in the cyberspace domain are radically different from military operations in the other warfighting domains. For example, cyberspace is an artificial construct and does not primarily exist in the natural world, while the other domains exist in nature. Cyberwar/NETWAR will primarily be fought over network terrain that is owned and operated by private sector entities, many of them multinational corporations. Military operations in the cyberspace domain simultaneously include physical and logical maneuver space. Cyberspace is a vastly shifting landscape compared to the other domains:

Cyberspace is dynamic and continually evolving. Changes in cyberspace are driven in large part by private industry research and development. The interdependency and innovation of civilian economic markets and communications industries have a direct impact on cybersecurity and military effectiveness. The domain itself is expanding and evolving as information technology and the market expand and evolve. In other words, portions of cyberspace continuously change due to technical innovation, including the addition, removal, replacement, or reconfiguration of components, and network protocols.[8]

Cyberspace is also one of the leading investment opportunities for the private sector.[9] For these reasons, it has intricate, undefined, and extremely challenging legal implications.

Far more than in the other warfighting domains, offensive warfare is dominant in the cyberspace domain.[10] Red Teams historically penetrate all ".mil" network defenses, at a nominal cost compared to the huge expense of creating and maintaining network defense. For example, if a particular server has 100 potential vulnerabilities, and the network administrator performs Herculean efforts to patch 99 of them (99 percent success rate on patches), any decent Red Team will find that single unpatched vulnerability and take control of the box, rendering the entire defensive effort useless. As an analogy, consider the battles of Crecy (1346) and Agincourt (1415), where English longbowmen slaughtered the French knights charging them. Before these encounters, the dominant offensive form of Western warfare was in the figure of a mounted armored knight. A technology (the longbow) and an organization (disciplined English foot soldiers) reversed this trend by creating a major imbalance favoring the defensive form of warfare after centuries of domination by the offensive form. Cyberspace, however, has not undergone any technological or organizational revolution that changes the extreme dominance and inherent imbalance of offensive cyberwarfare.

Much of what is considered offensive cyberspace activity does not meet the criteria of "attack" in the other domains. Shutting down or massively corrupting data in critical financial, health, or power grid networks constitutes an attack on national sovereignty and may or may not justify a use-of-force response (a political rather than legal or technical decision). A cyberspace attack on a supervisory control and data acquisition (SCADA) system that results in casualties or a regional power failure could be considered a kinetic effect to an offensive cyberspace operation.

U.S. Navy (Nina Hughes)

U.S. Fleet Forces commander speaks during standup ceremony for Navy Cyber Forces

At the other end of the spectrum, actions such as pinging, browsing, or port scanning are often used simply for the effective functioning of DOD networks and cyberspace operations and may or may not have hostile intent. Additionally, the vast majority of malware, botnets, and network intrusions into DOD's networks are technically competitive measures, espionage, vandalism, or crimes that fall under the category of technical network defense responses or traditional law enforcement/counterintelligence functions. These are not attacks on U.S. sovereignty. In many cases, this type of attack would be better described as network *irritation* than as network *attack*. But this noise-level network irritation can disguise a host of more serious attacks and needs to be cleaned out.

Cyberspace, due to its potential, differs considerably from the other warfighting domains. Cyberspace weapons can be created by anyone and launched in almost complete anonymity—a high-school student cannot spend a few nights hunched over a keyboard and create an F–22 fighter but could create a cyberspace weapon that could potentially disrupt major corporate and military networks and cause physical havoc. Attribution is almost impossible across the cyberspace domain; while it is difficult to envision a major/conventional ground, sea, or air attack that cannot be attributed to a nation-state, it is practically impossible to achieve attribution of a nation-state cyberspace aggressor if it chose anonymity. Key to successful cyberwarfare is attribution, which becomes increasingly difficult with current technology and Internet network communications terrain. Few attackers are identified unless they "self-identify" or are caught discussing their exploits in an unsecured chat room or a social network site. Attributing responsibility for state-sponsored operations can be practically impossible.

Operations in cyberspace occur near the speed of light and in real time, and often can impact the entire spectrum of the cyberspace domain simultaneously without notice or intelligence indicators. In military planning concepts, operations in the cyberspace domain can move from phase zero (shaping operations) to phase two (seizing the initiative) or even to phase three (dominating) instantaneously and worldwide, with huge implications (strengths and vulnerabilities) for the United States, aggressor nations, and nonstate actors.[11] This instantaneous nature and the ability to attack the entire domain simultaneously are characteristics that potentially make the cyberspace domain a much more dangerous and vulnerable domain.

The United States has not achieved dominance in the cyberspace domain. We intuitively understand that we dominate all warfighting domains except cyber—and our national economy, livelihood, civilization, and culture are as dependent on it as our military. Cyberspace is the only domain without a primary Service as lead and the only domain in which DOD will not defend the U.S. homeland.[12] For example, if DOD defended the land domain in the same manner as cyberspace, a Russian land (amphibious/airborne) invasion of New Jersey would have to be fought by U.S. citizens and commercial entities with whatever weapons they happened to possess. DOD would only defend Fort Monmouth and Fort Dix.

Why Should USCYBERCOM Be a COCOM?

Unity of Command/Effort. Current DOD approaches to cyberwarfare are scattered and fragmented across the Services and agencies. The Services, Defense Information Systems Agency (DISA), National Security Agency, Intelligence Community, and many of the other COCOMs have unsynchronized cyberspace warfighting capabilities. Unifying DOD's cyberspace effort into a focused subunified command is a necessary first step, but creating a separate and distinct USCYBERCOM as a fully functioning COCOM would provide it with indispensable authority, responsibility, legitimacy, and visibility. This would enable a stronger unity of command/effort across DOD and greater influence across the entire U.S. Government. Since the United States does not dominate the cyberspace domain, establishing a full COCOM would provide greater authority and

a high-school student cannot spend a few nights hunched over a keyboard and create an F–22 fighter but could create a cyberspace weapon that could potentially disrupt major corporate and military networks

responsibility to address this glaring national weakness.[13] Because of the unique nature of the domain, no one Service is responsible for operations to protect national cyberspace (unlike the other domains); a full COCOM would be better resourced and have greater authority and responsibility to compensate for the lack of a specific Service lead. USCYBERCOM will require acquisition authority similar to that of U.S. Special Operations Command in order to unify and streamline the procurement of military cyberspace capabilities (tools/weapons and associated training, doctrine, and support systems) as opposed to each individual Service developing and fielding an uncoordinated and disjointed set of cyberspace capabilities. The fragmentation of the Government's efforts to define, govern, regulate, defend, exploit (for intelligence purposes), and conduct operations in the cyberspace domain is embodied in the proliferation of definitions of *cyberspace*.[14]

Synchronization. USSTRATCOM is tasked under the Unified Command Plan to direct the defense of the Global Information Grid[15] and synchronize cyberspace operations. As a subunified command, USCYBERCOM probably will have insufficient authority to fully synchronize across the Services and other COCOMs. For example, geographic COCOMs might decide in the future to conduct full-spectrum cyberspace operations within their geographic areas of responsibility (AORs). This approach is incompatible with the nature of cyberspace/NETWAR operations and would be in conflict with three postulations:

■ *Geographic COCOMs who wanted to use cyberspace weapons as part of a regional geopolitical and military decision process would be potentially wasting strategic, one-time-use assets on regional objectives*. Offensive, full-spectrum cyberspace weapons are strategic in nature: once used, knowledge of their specific capabilities spreads across the Internet, and opponents can then adjust their defenses. An excellent example is a weaponized "zero-day" exploit—that is, an attack against a specific vulnerability currently unknown to the Internet community. Use of this weapon is a one-time launch. The worldwide Internet community will be able to rapidly create defenses and write and implement software patches against it.

■ *The technical workings of the Internet argue for a centralized authority and responsibility for potential offensive cyberspace operations*. If a specific geographic COCOM decides to launch a cyberspace offensive weapon from its location directly against a particular country (or a nonstate target within a country) in its AOR, the nature of the Internet ensures that the actual packets would cross routers, switches, and networks in countries outside the COCOM AOR. Packets often end up relayed by satellites across multiple continents. The attack cannot be confined to a direct line between the COCOM and the targeted country, and backscatter and blind retaliation may occur. These attacks would cross and impact other geographic COCOM AORs.

■ *The potential exists for certain attacks or types of cyberspace weapon to get out of control once launched*. The original Robert Morris worm in 1988 was not intended to take the Internet down, but it almost did. A cyberspace action taken by a geographic COCOM has a strong probability of impacting other geographic COCOMs and could have global implications. The potential unintended consequences of launching various cyberspace weapons argue for centralized command, control, and release authority.[16]

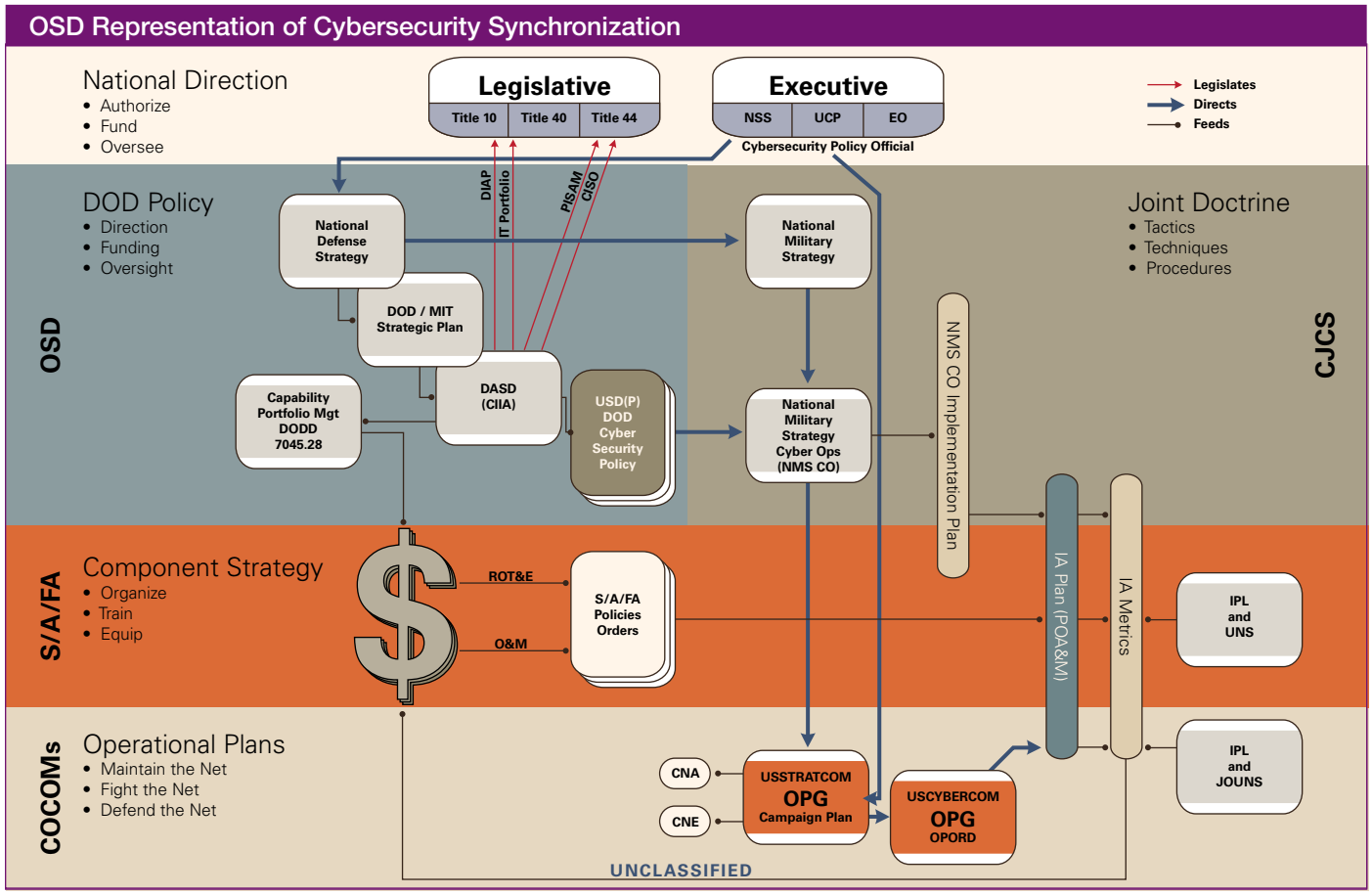
Mass. At least 13 different doctrinal documents at the OSD, DOD, agency, Service, and USSTRATCOM levels outline how DOD will fight a cyberwar. A central COCOM with exclusive authority and responsibility to conduct and synchronize cyberspace operations should consolidate the varied works into a concise doctrinal template from which DOD can conduct cyberspace operations. Each Service has its own doctrine and capability to conduct military operations in cyberspace.[17] Cyberwar/NETWAR capabilities need to be massed into one coordinated and synchronized set of strategic operations in order to achieve the intended massed effects. All aspects of cyberspace domain operations (defense, offense, network operations, and intelligence) need to be closely synchronized to eliminate any possible gaps or seams in the overall cyberspace posture.

Offensive Operations. The offensive form of cyberspace operations is far superior to the defensive form. DOD and the U.S. Government need to place more emphasis on the offensive form of full-spectrum cyberwar to support and ensure an appropriate defense. They must be prepared to answer cyberspace incidents with technical and nontechnical means of response and retaliation—preemptive or responsive actions across the diplomatic, informational, military, and economic spectrum to retaliate against aggressors and deter potential adversaries.

the potential unintended consequences of launching various cyberspace weapons argue for centralized authority

Diverse Mission Focus. The Obama administration has made limited attempts to protect the Nation from cyberspace threats,[18] but there are several national issues that require greater attention. Each Federal organization is focused on its individual mission area and responsibilities regarding cyberspace operations. The Obama administration decision to appoint a "Cyber Czar" (to organize the fragmented Federal Government cyberspace capabilities into a coherent and synchronized element) is a step in the right direction. However, the decision was clearly a low priority to the administration, and the position appears to lack the authority to properly focus and discipline the contentious Federal agencies on cyberspace domain concerns. This lack of central control has resulted in loose policy oversight by the Office of Management and Budget, OSD, Department of Homeland Security, and Department of Justice in their respective cyberspace responsibilities and capabilities, with weak or nonexistent policy compliance mechanisms. Additionally, divided Federal funding lines lead to more fragmentation of operational and command authority. Each department/Service/agency receives its own funding for information technology (IT)/cyberspace operations and purchases its own equipment (resulting in a failure of not only compatibility, information-sharing, and security, but also in the ability to leverage government buying power). Resource and performance metrics in cyberspace are weak or nonexistent. Cyberspace base funding in DOD (cutting across IT and information operations budgets but also found in electronic warfare and force protection budgets) is supplemented in an uncoordinated and fragmented fashion from the Comprehensive National Cyberspace Initiative,[19] and many other initiatives such as the OSD/DISA CyberCampaign Plan. The figure illustrates and provides details concerning DOD efforts to synchronize cyberspace security authority and resources.

There is a compelling requirement for a central DOD organization with the capability and authority to command and control, coordinate, and synchronize cyberwar/NETWAR functions at least across DOD, and possibly across the entire U.S. Government and the Nation at large. The coordination and synchronization mission for this command is critical—the Internet reaches across the entire modern enterprise. It touches not just those connected to it, but also those who are unaware how their lives are governed by technology. Every individual, every government, and every nation-state has a stake in the process. The technologies and domain environmental characteristics involved with cyberwar/NETWAR are strategic in nature, worldwide in scope, and overwhelmingly dominated by the offensive form of warfare—all leading to the requirement for centralized DOD and U.S. Government authority. The network terrain over which cyberwar/NETWAR will be conducted is radically different from the physical world of other warfighting domains in that it can affect not only that which is "network" but also that which is "network controlled"—life-support systems, SCADA, physical infrastructure, and so forth. The cyber domain is sufficiently different from other warfighting domains that it requires a command with the requisite authority, responsibilities, and resources to successfully conduct DOD's full-spectrum cyberwar/NETWAR operations with the understanding that the mission of the Defense Department is the defense of the Nation, regardless of domain. The DOD solution needs to be the establishment of a subunified command with the goal of a full combatant command in the near future. The requirement for a central authority to conduct cyberdefense/cyberwar/NETWAR is time-critical due to glaring network defensive vulnerabilities, the potential for disastrous consequences for the Defense Department's global network and the national/global Internet, the potential destruction of the national infrastructure, and the lives of U.S. citizens. These threats are even more critical due to the instantaneous nature of the Internet. As DOD facilitates economic globalization and



Source: OSD Defense Information Assurance Program briefing on USCYBERCOM standup, by author.

Key: CISO = Chief Information Security Officer; CJCS = Chairman of the Joint Chiefs of Staff; CNA = Computer Network Attack; CNE = Computer Network Exploitation; COCOM = Combatant Command; DASD (CIIA) = Deputy Assistant Secretary of Defense (Cyber, Information, and Identity Assurance) (under the Assistant Secretary of Defense [Networks and Information Integration]/DOD Chief Information Officer); DIAP = Defense Information Assurance Program; DOD = Department of Defense; DODD = Department of Defense Directive; EO = Executive Order; IA = Information Assurance; IMIT = Information Management Information Technology; IPL = Integrated Priority List; JOUNS = Joint Operations Urgency of Need Statement; NMS CO = 2006 National Military Strategy for Cyberspace Operations; NSS = National Security Strategy; O&M = Operations and Maintenance; OPG = Operations Planning Group; OPORD = Operation Order; OSD = Office of the Secretary of Defense; POA&M = Plans of Action and Milestones; RDT&E = Research, Development, Testing, and Evaluation; S/A/FA = Services/Agencies/Field Activity; UCP = Unified Command Plan; UNS = Urgency of Need Statement; USD(P) = Under Secretary of Defense for Policy.

international trade in the physical realm (for example, the U.S. Navy provides security to international maritime traffic), it is also the only organization that can perform similar security operations in the virtual Internet realm. It is clearly in our national interest to secure and dominate the cyberspace environment.

Current DOD and U.S. Government efforts to conduct cyberdefense/cyberwar/NETWAR are badly fragmented and require greater central authority and integration/synchronization of overall cyberspace operations. Resources to defend the national strategic portions of the cyberspace domain are woefully inadequate, and many of the resources are acquired and deployed in an unfocused and uncoordinated fashion. The development of a subunified command is a necessary first step toward resolving these issues. It provides an effective tradeoff between the time required to develop a central cyberwar organization and the immediate need to provision that organization with the authority to properly command and control, synchronize, and coordinate DOD's cyberdefense/cyberwar/NETWAR operations.

The subunified command can be developed and made operational more quickly than a full COCOM, yet it has many of the same authorities, roles, missions, and responsibilities. It has the same skeletal structure as a full COCOM with reduced capabilities. The next logical step is to use the subunified command as a core to launch a full combatant command to extend the resources and authority of USCYBERCOM to the essential level of authority and effectiveness. Cyberspace is a contested domain, and the United States needs sovereign options to defend itself and its global interests; to deter, dissuade, disrupt, deny, and defeat our adversaries; and to protect our national (economic, military, cultural, and social) interests. **JFQ**

NOTES

[1] Michael Posner, "America already is in a cyber war, analyst says," *Government Executive*, November 27, 2007, available at <www.govexec.com/dailyfed/1107/112707tdpm2.htm>. Also see Clifford May, "The E-Jihad," *National Review* blog posting, October 20, 2009.

[2] U.S. Army Combined Arms Center, *The United States Army Concept of Operation (CONOPS) for Cyber-Electronics (C-E) 2010–2024*, author's draft, version 0.1, March 4, 2009, 14: "For C-E, NETWAR is the integrated use of computer network attack (CNA), computer network exploitation (CNE), space control (SC), electronic attack (EA), electronic warfare support (ES), and physical attack. It is supported by intelligence and creates both physical and cognitive effects."

[3] Wyatt Kash, "Cyber command in urgent need of strategy, military leaders say: Military leaders expect new command to articulate its strategy soon," *Federal Computer Week*, June 30, 2009, available at <www.fcw.com/Articles/2009/06/30/Military-leaders-Cyber-Command-strategy.aspx >. See also Bob Brewin, "Battlespace," *Government Executive*, 2008, available at <www.govexec.com/dailyfed/1008/101308wb.htm?rss=getoday>, and the Center for Strategic and International Studies, "Report of the CSIS Commission on Cybersecurity for the 44th Presidency," 2008, available at <http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf>, 48.

[4] William Gibson first defined *cyberspace* in his 1984 science fiction novel *Neuromancer.*

[5] Chairman of the Joint Chiefs of Staff, *2006 National Military Strategy for Cyberspace Operations*, available at <www.DOD.mil/pubs/foi/ojcs/072105doc1.pdf>.

[6] White House, National Security Council, *2003 National Strategy to Secure Cyberspace*, 2003, available at <www.dhs.gov/xprevprot/programs/editorial_0329.shtm>.

[7] U.S. Air Force Cyberspace Command, *Strategic Vision 2008*, available at <www.afcyber.af.mil/shared/media/document/AFD-080303-054.pdf>; David Fahrenkrug, "Cyberspace Defined," Air University, available at <www.au.af.mil/au/aunews/archive/0209/Articles/CyberspaceDefined.html>; Office of the Secretary of Defense Policy Memorandum, "Cyberspace Operations," 2008, available at <http://afei.org.documents/newcyberdefinition.pdf>; "Memorandum for Secretaries of Military Departments, Subject: The Definition of Cyberspace," 2008; Dan Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," available at <www.carlisle.army.mil/DIME/documents/Cyber%20Chapter%20Kuehl%20Final.doc>.

[8] The *United States Army Concept of Operation* on page 10 also contains an excellent example of cyberspace as both logical and physical maneuver space utilized simultaneously.

[9] Lisa Springer, "Cyber Security: The Next Great Defense Opportunity," *Investor Ideas* (June 16, 2009), available at <www.investorideas.com/News/061609A.asp>. Also see C. Drew and J. Markoff, "Contractors Vie for Plum Work Hacking for U.S.," *The New York Times*, May 31, 2009; and Gopal Ratnam, "Lockheed, Boeing Tap $11 Billion Cybersecurity Market," *Bloomberg Information*, available at <www.bloomberg.com/apps/news?pid=20601103&sid=an2_Z6u1JPGw>.

[10] *Strategic Vision 2008*.

[11] For a more detailed description of the six planning phases, see Joint Chiefs of Staff, Joint Publication 5–0, *Joint Operation Planning*, 2006, available at <www.dtic.mil/doctrine/new_pubs/jp5_0.pdf>.

[12] Some thought has been given to DOD defense of civilian networks; see Ellen Nakashima, "Cyber-Command May Help Protect Civilian Networks," *The Washington Post*, May 5, 2009.

[13] STRATFOR, "U.S. Strengthening Cybersecurity," 2008, available at <www.stratfor.com/analysis/u_s_strengthening_cybersecurity>.

[14] Wyatt Kash, "Report on House Homeland Security Subcommittee Hearings," *Government Computer News*, September 29, 2008, available at <http://gcn.com/Articles/2008/09/26/Wyatt-Kash--Elevate-cybersecurity.aspx>.

[15] Department of Defense Directive 8100.1, *Global Information Grid (GIG) Overarching Policy*, September 19, 2002, available at <http://biotech.law.lsu.edu/blaw/DODd/corres/pdf/d81001_091902/d81001p.pdf>.

[16] RAND, "Turning Density to Advantage: C4ISR and Information Operations as Examples," and J.S. Monroe, "Cyber Command: Observers worry about unintended consequences: DOD, NSA offer formidable pairing, experts say," *Federal Computer Week*, June 25, 2009, available at <www.fcw.com/Articles/2009/06/25/cyber-command-DOD-NSA.aspx>.

[17] See Noah Shachtman, "U.S. Cyber Command: 404 Error, Mission Not (Yet) Found," *Wired.com*, June 2009, available at <www.wired.com/dangerroom/2009/06/foggy-future-for-militarys-new-cyber-command/>; and Mark Hosenball, "The Turf War over Cyberwar," *Newsweek*, April 25, 2009, available at <www.newsweek.com/id/195107>.

[18] The White House, "White House Efforts to Protect Our Information Networks," available at <www.whitehouse.gov/agenda/homeland_security/>.

[19] Department of Homeland Security, "Fact sheet: Protecting our Federal Networks against Cyber Attacks," available at <www.dhs.gov/xnews/releases/pr_1207684277498.shtm>. STRATFOR, "Cyberwarfare," July 21, 2008, available at <www.stratfor.com/analysis/u_s_strengthening_cybersecurity>.